Electronic Colloquium on Computational Complexity, Report No. 326 (2026)

Möbius-Pseudorandomness for Algebraic Circuits

Gil Kalai* Mrinal Kumar† Ben Lee Volk‡

Abstract

We define a notion of Möbius-pseudorandomness for integer sequences generated by multivariate polynomials computed by small and simple algebraic circuits. This mirrors a related definition of Kalai that concerns boolean functions computed by small boolean circuits.

We then prove Möbius-pseudorandomness results for polynomials computed by algebraic circuits with few multiplication gates (of any depth), for polynomials with small-dimensional partial derivative space, and for the determinant and permanent. We conjecture that these results hold in general for polynomial-size algebraic circuits.

1 Introduction

1.1 Möbius-Pseudorandomness

Recall that the Möbius function $\mu : \mathbb{N} \to \{-1, 0, 1\}$ is defined as follows: $\mu(m) = 0$ if m isn't square-free, and $\mu(m) = (-1)^k$ if m is square-free and the number of its prime factors is k.

A sequence $\{a_n\}_{n\in\mathbb{N}}$ is said to be *Möbius-pseudorandom* if it has vanishingly small correlation with the Möbius function. More formally:

Definition 1.1. *Let $\{a_n\}_{n\in\mathbb{N}}$ be a bounded integer sequence (or more generally, a sequence of complex numbers). We say that it is* Möbius-pseudorandom *if*

$$\frac{1}{N}\left|\sum_{m=0}^{N-1}\mu(m)a_m\right| = o(1). \tag{1}$$

*Efi Arazi School of Computer Science, Reichman University and Einstein Institute of Mathematics, Hebrew University of Jerusalem. Email: gil.kalai@gmail.com. Supported by ERC grant 834735 and by an ISF grant 2669/21.

†Tata Institute of Fundamental Research, Mumbai, India. Email: mrinal@tifr.res.in. Research supported by the Department of Atomic Energy, Government of India, under project number RTI400112, and in part by Google and Premji Invest Research Grants.

‡Efi Arazi School of Computer Science, Reichman University, Israel. Email: benleevolk@gmail.com. The research leading to these results has received funding from the Israel Science Foundation (grant number 843/23).

ISSN 1433-8092

In what follows, it is slightly more convenient to sum over integers from 0 to $N-1$ and thus we may define arbitrarily $\mu(0) = 0$, as this clearly does not matter with respect to the pseudorandomness property.

Similarly, one can define a function to be *Liouville-pseudorandom* if the same holds with the Liouville function $\lambda(m)$ instead of $\mu(m)$. The Liouville function $\lambda : \mathbb{N} \to \{-1, 1\}$ is defined as $\lambda(m) = (-1)^k$ where k is the number of prime factors of m, counted with multiplicity. All the results and conjectures in this paper hold with respect to Liouville-pseudorandomness as well.

This notion of Möbius-pseudorandomness is well studied in number theory and in other areas,[1] and a significant amount of work was devoted to proving that certain sequences are Möbius-pseudorandom. Sarnak [Sar12] has made the following conjecture:

Conjecture 1.2 (Sarnak's conjecture)**.** *Every deterministic bounded sequence is Möbius-pseudorandom.*

The notion of a "deterministic sequence" arises from topological dynamics. For Boolean sequences $f(n), n \in \mathbb{N}$, the definition is especially simple: f is "deterministic" if the number of patterns

$$(f(n+1), f(n+2), \ldots, f(n+m)) : n \in \mathbb{N}$$

is $\exp(o(m))$. See [Sar12] for the general definition. (For the case of general bounded functions f the condition is that for every real $\epsilon > 0$ all these patterns can be covered by $\exp(o(m))$ balls of radius ϵ in the ℓ_∞ metric.)

There is a variety of classes of sequences for which Möbius-pseudorandomness holds, including various special cases of Sarnak's Conjecture 1.2. For example, the following classical theorem goes back to Davenport.

Theorem 1.3 ([Dav37, Hua65])**.** *(i) For an irrational number α, the sequence $f(n) = e^{\pi i \alpha n}$ is Möbius-pseudorandom.*

(ii) For a polynomial $p(n)$ the sequence $f(n) = e^{\pi i \alpha p(n)}$ is Möbius-pseudorandom.

A far-reaching extension of Davenport's theorem was proved by Green and Tao [GT12]. For another important special case of Sarnak's conjecture see Bourgain, Sarnak, and Ziegler [BSZ12] and the surveys [FKPL18, Zie26]. A general result about *automatic sequences* was proved by Müllner [Mül17].

1.2 Computational complexity and Möbius pseudorandomness

Sarnak [Sar10, Sar12] raised the question of whether every function that can be computed in polynomial time is Möbius-pseudorandom. Here, in order to make sense of the

[1] It is often called there *Möbius-randomness*. However, borrowing the standard terminology of computational complexity theory, we prefer to use "pseudorandomness" rather than "randomness" as neither the Möbius function nor the sequence we consider are truly random; rather, we investigate the amount to which such sequences correlate with the Möbius function.

question one needs to fix an encoding of integers. It is natural to consider integers encoded using binary digits, and therefore the assumption that the function is computed in polynomial time means that there exists a polynomial time algorithm that given the binary digits of m computes $f(m)$, in time which is polynomial in the number of binary digits of m. To that end, we introduce some notation. For an integer $m < N = 2^n$ let $(m_1, \ldots, m_n)$ denote its binary digits.

Definition 1.4 (Möbius-pseudorandomness of Boolean Functions)**.** *Let $f = \{f_n\}_{n\in\mathbb{N}}$ be a sequence of n-variate boolean functions. We say f is* Möbius-pseudorandom *if*

$$\frac{1}{N}\left|\sum_{m=0}^{N-1}\mu(m)\exp(i\pi\cdot f_n(m_1,\ldots,m_n))\right| = o(1)$$

where $N = 2^n$ and $(m_1, \ldots, m_n)$ are the binary digits of the integer m.

We may then consider the complexity of the sequence of functions $\{f_n\}_{n\in\mathbb{N}}$ where $f_n(x_1, \ldots, x_n)$ outputs, on input $m_1, \ldots, m_n$, the integer $f_n(m)$. f_n is efficiently computable if this computation can be done in time polynomial in n. Here one may consider either non-uniform computation (using circuits) or uniform computation (in which there exists a single Turing machine that computes $f_n(m)$ for every n and m).

Sarnak, however, expected a negative answer to his conjecture, since he expressed his belief that efficient algorithms for integer factoring, and hence for computing μ do exist. For completeness, we state here a strong form of a positive answer to Sarnak's question.

Conjecture 1.5. *Every polynomial-time computable function f is Möbius-pseudorandom.*

Conjecture 1.5, while plausible, is even stronger than the assertion that there is no polynomial-time factoring algorithm (which is considerably stronger than the $\mathbf{P} \neq \mathbf{NP}$ conjecture).

Kalai initiated a line of work whose purpose is to study Sarnak's conjecture for various limited complexity classes. The goal is to offer computational complexity conjectures or theorems that on the one hand use computational classes that can be shown to be limited by current techniques (like bounded depth circuits, although we note that sequences represented by bounded depth circuits need not be *deterministic* in the sense of Conjecture 1.2), and on the other hand, may include concrete classes of functions that occurred naturally in number theory. A far-reaching goal would be to find computational complexity setting that is rich enough to include many concrete results about Möbius-pseudorandomness from number theory. It seems that arithmetic formulas and circuits could be especially relevant.

Following Kalai's [Kal11] suggestion, Möbius-pseudorandomness results were proved for various complexity classes.

Green [Gre12] has proved that boolean functions in AC^0 are Möbius-pseudorandom by estimating the low-degree Fourier-Walsh coefficients of the Möbius function. Bourgain [Bou13b, Bou13a, Bou16] obtained some improved estimates on the Fourier-Walsh coefficients, that also allowed him to prove that *monotone* boolean functions

are Möbius-pseudorandom. We give more details on Bourgain's results in Section 2, as his results are very relevant to ours.

Extending these results to larger complexity classes is an open problem. We record two conjectures in that regard:

Conjecture 1.6 (Möbius-pseudorandomness conjecture for $\mathsf{AC}^0(p)$)**.** *Let p be a fixed prime. Suppose $f = \{f_n\}_{n\in\mathbb{N}}$ is in $\mathsf{AC}^0(p)$, that is, it can be computed by a polynomial size bounded depth Boolean circuit with* mod p *gates. Then f is Möbius-pseudorandom.*

Conjecture 1.7 (Möbius-pseudorandomness conjecture for low degree polynomials)**.** *Suppose f can be represented by a polynomial over $\mathbb{Z}/p\mathbb{Z}$ of degree at most* polylog(n)*: that is, there exists an n-variate polynomial P over $\mathbb{Z}/p\mathbb{Z}$, of degree at most* polylog(n)*, such that for every $x \in \{0,1\}^n$, $f(x) = P(x)$. Then f is Möbius-pseudorandom.*

An important theorem by Razborov and Smolensky [Raz87, Smo87, Smo93] implies that Conjecture 1.7 implies Conjecture 1.6.

We remark that Conjecture 1.7 is known to hold for *linear* polynomials, by Bourgain's result on the Fourier-Walsh coefficients mentioned above. A special case of degree-2 polynomials is Möbius-pseudorandomness for the Rudin-Shapiro sequence. This case was settled by Tao [Tao12] who relies on the Katai-Bourgain-Sarnak-Ziegler orthogonality criterion.

One should also note the difference between Conjecture 1.7, which refers to low-degree boolean functions in the binary digits of an integer n, with degree that can possibly grow with n, and Theorem 1.3, that deals with polynomials in n (of fixed degree).

1.3 Möbius-Pseudorandomness in Algebraic Complexity

Similar to the boolean case, one could consider sequences that can be encoded using "simple" objects in algebraic complexity theory, which studies the computation of polynomials using arithmetic operations. Our goal in this note is to propose some conjectures along these lines, and prove some special cases of them.

Definition 1.8 (Möbius-pseudorandomness for polynomials)**.** *Let $f = \{f_n\}_{n\in\mathbb{N}}$ be a sequence of n-variate integer polynomials. We say f is* Möbius-pseudorandom *if*

$$\frac{1}{N}\left|\sum_{m=0}^{N-1}\mu(m)\exp(i\pi\cdot f_n(m_1,\ldots,m_n))\right| = o(1)$$

where $N = 2^n$ and $(m_1,\ldots,m_n)$ are the binary digits of the integer m.

For readers versed in algebraic complexity theory, our choice to focus on *evaluations* of the polynomial over boolean inputs may seem odd: Since algebraic complexity theorists are usually concerned with polynomials as formal objects (rather than the functions that they compute) it might seem natural to focus on the sequence of *coefficients* of such polynomials. However, despite considerable efforts and multiple iterations, we were unable to find a general enough "coefficient version" of Definition 1.8 that makes

sense. A natural attempt would be to look at the coefficient sequence of multilinear polynomials, but then the $\frac{1}{N}$ normalization in Definition 1.8 would imply that any homogeneous multilinear polynomial will be Möbius-pseudorandom, regardless of its complexity, as most of its coefficients will be 0. Different normalizations then lead to trivial constructions of such polynomials that correlate well with the Möbius function, especially since algebraic circuits are a non-uniform model of computation.

1.4 Our Results

In this paper we prove Möbius-pseudorandomness for certain classes of polynomials computed by small algebraic circuits in various models.

Theorem 1.9. *The following classes of polynomials are Möbius-pseudorandom:*

- *Polynomials computed by depth-3 circuits of top fan-in $o(n)$ (Section 3)*
- *Polynomials whose first-order partial derivatives span a space of dimension $o(n)$ (Section 4)*
- *Polynomials computed by circuits with $o(n)$ multiplication gates (Section 5).*

The definitions of the corresponding models appear in the relevant sections.

In addition, in Section 6, we prove that the determinant and permanent polynomials, the most important polynomials in algebraic complexity, are Möbius-pseudorandom as well.

In the spirit of Conjecture 1.5, we conjecture that such results hold in much greater generality than what we are able to prove.

1.5 Techniques

The main tool we use is a strong correlation bound by Bourgain [Bou13a] that bounds the correlation of the Möbius function with Fourier-Walsh characters over $\mathbb{F}_2$. As mentioned in Section 1.2, such a bound can be used to show that boolean functions in AC^0, and monotone boolean functions, are Möbius-pseudorandom. It is perhaps slightly more surprising that this bound also has applications for showing Möbius-pseudorandomness for *algebraic* circuits. However, it turns out that in many settings if $f(\mathbf{x})$ is an integer polynomial computed by some limited class of circuits, we are able to give an upper bound on the algebra norm (that is, the L_1 norm of the Fourier-Walsh transform) of the boolean function $(-1)^f$. Such bounds, combined with Bourgain's [Bou13a] correlation upper bound as well as the estimates of [Bou16], imply that those polynomials are Möbius-pseudorandom.

For the determinant polynomial, the situation is slightly more complicated. However, here we are able to prove that the determinant modulo 2 can be *approximated* (in L_2 norm) by a function with small Fourier-Walsh L_1 norm, which is sufficient for the argument to go through.

2 Preliminaries

In this section we state some preliminary results that will be used in the next sections.

As mentioned in Section 1.5, Bourgain [Bou13a, Bou13b, Bou16] (following Green [Gre12]) has obtained several bounds on the Fourier-Walsh coefficients of the Möbius function. In particular, [Bou13a] provides a uniform $2^{-n^{1/10}}$ upper bound on the magnitude of each such coefficient. However, considering low-degree and high-degree coefficients separately slightly improves the parameters in our results.

The following lemma obtains an improved estimate for high-degree coefficients. Its proof is implicit in [Bou13a]. Since the exact statement does not appear in [Bou13a], we detail some of the calculations.

Lemma 2.1 (Implicit in [Bou13a])**.** *Let $\chi_S : \mathbb{F}_2^n \to \{-1,1\}$ be a Fourier-Walsh character of $\mathbb{F}_2^n$ corresponding to $S \subseteq [n]$ that is, $\chi_S(x) = (-1)^{\sum_{i\in S} x_i}$. If $|S| \geq \sqrt{n}\log^2 n$, then there exists an absolute constant $\delta > 0$ such that, for sufficiently large n,*

$$\frac{1}{N}\left|\sum_{m=0}^{N-1} \mu(m)\chi_S(m_1,\ldots,m_n)\right| \leq 2^{-\delta|S|^2/n}$$

where $N = 2^n$.

Proof. Fix S with $|S| = t$ and set $h = t^2/n$.

Following the proof in [Bou13a] (see also Lemma 1 of [MR10]), we need to bound the so-called Type-I and Type-II sums.

Set $M_0 = 2^{at}$ and $L = 2^{bh}$, where $a > 0$ is a small constant and $b > 0$ is sufficiently small with respect to a. For $M \geq M_0$, Bourgain's [Bou13a] Equation 2.31 upper bounds Type-II sums by

$$T_{\mathrm{II}} \leq N\left(L^{-c_1} + L^2 M^{-c_2} + L^C 2^{-c_3 \log_2 M|S|/n}\right)$$

where c_1, c_2, c_3, C are absolute constants (with Bourgain's [Bou13a] parameter ε fixed). Using the assumptions on M and L,

$$T_{\mathrm{II}} \leq N\left(2^{-c_1 bh} + 2^{2bh - c_2 at} + 2^{(Cb - c_3 a)h}\right),$$

where in the third summand we used the fact that $h = t^2/n$. Since $h \leq t$, we get that

$$T_{\mathrm{II}} \leq N \cdot 2^{-\delta h}$$

for some $\delta > 0$.

The parameter restrictions preceding (2.3) in [Bou13a] hold: writing $u = \log_2 M$ and $\rho = \log_2 L = bh$, we have that for large enough n,

$$\log^2 n \ll \rho < u/100,$$

since $h = t^2/n \geq \log^4 n$ and $u/100 \geq at/100 > bh$, since $h \leq t$ and b can be picked sufficiently small with respect to a.

For $M \le M_0$, Type-I sums are upper bounded in equations (3.2′) and (1.3) of [Bou13a], that give the upper bound

$$T_{\mathrm{I}} \le Nn^2 M 2^{-c_0|S|} \le Nn^2\, 2^{(a-c_0)t} \le Nn^2\, 2^{-c_0 t/2},$$

if $a < c_0/2$.

The bounds on Type-I and Type-II sums now imply

$$\left|\sum_{m=0}^{N-1} \mu(m)\chi_S(m_1,\ldots,m_n)\right| \le N \cdot n^{O(1)} \cdot 2^{-\delta' h} \le N \cdot 2^{-\delta h}$$

for some constants $\delta', \delta > 0$ (since $h \ge \log^4 n$, the polynomial factor can be comfortably absorbed by choosing a slightly smaller $0 < \delta < \delta'$). □

We also require the following estimate by Bourgain [Bou16] on the total mass of the low-degree Fourier-Walsh coefficients of the Möbius function.

Theorem 2.2. *Let $\{\hat{\mu}(S) : S \subseteq [n]\}$ denote the Fourier-Walsh coefficients of the Möbius function μ (thought of as a function $\mu : \{0,1\}^n \to \{-1,0,1\}$ whose input is the binary digits of an integer). Then there exists a constant $\rho > 0$ such that for every constant C,*

$$\sum_{A \subseteq [n], |A| \le \rho n} \hat{\mu}(A)^2 \le n^{-C}.$$

For a function $f : \mathbb{F}_2^n \to \mathbb{R}$ we denote by $\left\{\hat{f}(S)\right\}_{S\subseteq[n]}$ its Fourier-Walsh coefficients, and by $\|f\|_A$ its *algebra norm* (or L_1 norm), $\|f\|_A = \sum_{S\subseteq[n]} |\hat{f}(S)|$. It holds that $\|f \cdot g\|_A \le \|f\|_A \cdot \|g\|_A$.

We further define $\|f\|_2 = \left(\mathbb{E}_x[f(x)^2]\right)^{1/2}$ where the expectation is over a uniformly random x.

The following lemma gives an upper bound on the correlation of a function with small algebra norm with the Möbius function.

Lemma 2.3. *There exists a universal constant $\varepsilon > 0$ with the following property: Let $f : \mathbb{F}_2^n \to \mathbb{R}$ be a function with $\|f\|_2 \le 1$, and suppose that $\|f\|_A \le 2^{\varepsilon n}$. Then*

$$\frac{1}{N}\left|\sum_{m=0}^{N-1} \mu(m) f(m_1,\ldots,m_n)\right| = o(1)$$

(where $N = 2^n$ and $(m_1,\ldots,m_n)$ are the binary digits of the integer m).

A weaker form of Lemma 2.3 in which the assumption $\|f\|_A \le 2^{\varepsilon n}$ is replaced by $\|f\|_A \le 2^{\varepsilon n^{1/10}}$ can be directly deduced from the main theorem of [Bou13a], that gives a uniform upper bound on the correlation of μ with any Fourier-Walsh character. However, by exploiting Theorem 2.2 and the improved correlation upper bound from Lemma 2.1, we are able to obtain the stronger version. Note that by Cauchy-Schwarz, any boolean function has $\|f\|_A \le 2^{n/2}$.

Proof. We think of μ as a function $\mu : \mathbb{F}_2^n \to \{-1, 0, 1\}$ by identifying an integer $m \in [0, 2^n - 1]$ with its binary digits. The Fourier-Walsh coefficients of f and μ are then denoted $\hat{f}(S), \hat{\mu}(S)$ for $S \subseteq [n]$, respectively. Expanding both functions in the Fourier basis and using the orthonormality of the Fourier characters, we obtain

$$\begin{aligned}\left|\frac{1}{N}\sum_{m=0}^{N-1}\mu(m_1,\ldots,m_n)f(m_1,\ldots,m_n)\right| &= \left|\sum_{S\subseteq[n]}\hat{f}(S)\hat{\mu}(S)\right| \\ &\leq \left|\sum_{|S|\leq\rho n}\hat{f}(S)\hat{\mu}(S)\right| + \left|\sum_{|S|>\rho n}\hat{f}(S)\hat{\mu}(S)\right|.\end{aligned}$$

Here ρ is a small constant to be picked later. By Cauchy-Schwarz, we can upper bound the right hand side by

$$\left(\sum_{|S|\leq\rho n}\hat{f}(S)^2\right)^{1/2}\cdot\left(\sum_{|S|\leq\rho n}\hat{\mu}(S)^2\right)^{1/2} + \max_{S\subseteq[n],|S|>\rho n}|\hat{\mu}(S)|\cdot\left(\sum_{|S|>\rho n}|\hat{f}(S)|\right). \quad (2)$$

The assumption $\|f\|_2 \leq 1$ and Parseval's identity, along with Theorem 2.2, imply that the first term in (2) is upper bounded by n^{-C} for any constant C, assuming ρ is picked to be a small enough constant to apply Theorem 2.2.

Lemma 2.1 and the assumption on $\|f\|_A$ imply that the second term is at most

$$2^{-\delta\rho^2 n}\cdot 2^{\varepsilon n}$$

where δ is a small constant (depending on ρ). Picking $\varepsilon = \delta\rho^2/2$ finishes the proof. □

3 Depth-3 Formulas

In the same spirit of Kalai's conjecture, and the results of Green [Gre12] and Bourgain [Bou13b, Bou16, Bou13a], we conjecture that "simple" polynomials are Möbius-pseudorandom, where simplicity is measured with respect to low algebraic complexity. Such results were not previously known even for very simple algebraic models.

Definition 3.1. *Let $f \in \mathbb{Z}[\mathbf{x}]$ be an n-variate multilinear polynomial. We say f is computed by a depth-3 formula of top fan-in s over $\mathbb{Z}$ if*

$$f = \sum_{i=1}^{s}\prod_{j=1}^{d_i}\ell_{i,j}(x_1,\ldots,x_n)$$

where for every i, j, $\ell_{i,j} \in \mathbb{Z}[\mathbf{x}]$ is a linear function with integral coefficients.

There are some natural submodels of depth-3 formulas. Recall that we assume f is a multilinear polynomial. If, for every i, the linear functions $\ell_{i_1}, \ldots, \ell_{i,d_i}$ are variable disjoint, the formula is called a *depth-3 multilinear formula*.

One may even further restrict to *set-multilinear formulas*, defined as follows. Let $\mathbf{x} = (x_1, \ldots, x_n)$ denote a tuple of n variables. A polynomial $f \in \mathbb{Z}[\mathbf{x}]$ is called *set-multilinear* if there exists a partition of $\mathbf{x}$ into d sets $\mathbf{x}_1, \ldots, \mathbf{x}_d$, and every monomial with non-zero coefficient in f is of the form $\prod_{i=1}^{d} x_{i,j_i}$ with $x_{i,j_i} \in \mathbf{x}_i$.

If we denote $n_i := |\mathbf{x}_i|$ and $\mathbf{x}_i = (x_{i,1}, \ldots, x_{i,n_i})$, there is a natural correspondence between such polynomials and d-dimensional tensors of format $n_1 \times n_2 \times \cdots \times n_d$ (the $(i_1, \ldots, i_d)$ entry of the tensor is the coefficient of $x_{1,i_1} x_{2,i_2} \cdots x_{d,i_d}$).

A tensor of rank one corresponds to a set-multilinear polynomial of the form

$$\ell_1(\mathbf{x}_1) \cdot \ell_2(\mathbf{x}_2) \cdots \ell_d(\mathbf{x}_d),$$

where for every $1 \le i \le d$, ℓ_i is a linear function in the variables of $\mathbf{x}_i$.

Definition 3.2 (Set Multilinear Formulas of Depth 3)**.** *Let $f \in \mathbb{Z}[\mathbf{x}]$ be a set-multilinear polynomial with respect to the partition $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_d)$. We say f is computed by a set-multilinear formula of depth 3 and top fan-in s over $\mathbb{Z}$ if*

$$f = \sum_{i=1}^{s} \prod_{j=1}^{d} \ell_{i,j}(\mathbf{x}_j),$$

where for every $1 \le i \le s$ and $1 \le j \le d$, $\ell_{i,j}$ is a linear function with integral coefficients.

Set-multilinear polynomials computed by depth-3 formulas of top fan-in s correspond to tensors of rank at most s.

We first prove that small depth-3 formulas compute Möbius-pseudorandom polynomials as in Definition 1.8. Note that this proof does not even assume multilinearity or set-multilinearity of the formula.

Theorem 3.3. *Let $f = \{f_n\}_{n \in \mathbb{N}}$ be a sequence of integer polynomials computed by depth-3 formulas of top fan-in s, where $s \le \varepsilon n$ for some small constant $\varepsilon > 0$. Then f is Möbius-pseudorandom.*

Proof. Let

$$f(\mathbf{x}) = \sum_{i=1}^{s} P_i(x), \qquad P_i(\mathbf{x}) = \prod_{j=1}^{d_i} \ell_{i,j}(\mathbf{x}),$$

where each $\ell_{i,j}$ has integer coefficients.

Let $g_i(\mathbf{x}) = (-1)^{P_i(\mathbf{x})}$ and $\chi_{i,j}(\mathbf{x}) = (-1)^{\ell_{i,j}(\mathbf{x})}$. Each $\chi_{i,j}$ is a Fourier-Walsh character. Then, observe that

$$\begin{aligned} g_i(\mathbf{x}) &= 1 - 2 \prod_{j=1}^{d_i} \frac{1 - \chi_{i,j}(\mathbf{x})}{2} \\ &= 1 - 2^{1-d_i} \prod_{j=1}^{d_i} (1 - \chi_{i,j}(\mathbf{x})). \end{aligned}$$

Expanding the product and using the triangle inequality gives

$$\|g_i\|_A \leq 1 + 2^{1-d_i} \cdot 2^{d_i} = 3.$$

Since $(-1)^{f(x)} = \prod_{i=1}^{s} g_i(x)$, submultiplicativity yields

$$\left\|(-1)^f\right\|_A \leq \prod_{i=1}^{s} \|g_i\|_A \leq 3^s.$$

By Lemma 2.3, assuming $s \leq \varepsilon n$,

$$\frac{1}{N}\left|\sum_{m=0}^{N-1} \mu(m) \exp(i\pi f(m_1, \ldots, m_n))\right| = o(1). \qquad \square$$

4 Polynomials with Low-Dimensional Partial Derivatives

The method of partial derivatives is a common technique for proving lower bounds for various computational models.

Let $f \in \mathbb{F}[\mathbf{x}]$. Denote by ∂f the space of partial derivatives (of all orders) of f. The following properties, by [NW97], are easy to prove:

Claim 4.1 ([NW97]). *1. If $f = \ell^d$ where ℓ is a linear function, then $\dim \partial f \leq d+1$.*

2. If $f = \prod_{j=1}^{d} \ell_j(\mathbf{x}_j)$ where ℓ_j is a linear function for every $1 \leq j \leq d$, then $\dim \partial f \leq 2^d$.

3. $\dim \partial(f+g) \leq \dim \partial f + \dim \partial g$.

Therefore, if $f = \sum_{i=1}^{s} \ell_i^d$ then $\dim \partial f \leq (d+1)s$, and if $f = \sum_{i=1}^{s} \prod_{j=1}^{d} \ell_{i,j}(\mathbf{x}_j)$, it holds that $\dim \partial f \leq s \cdot 2^d$.

It follows that lower bounds on the dimension of the space of partial derivatives of f can be used to prove lower bounds on the minimal size of a depth-3 powering formula or a depth-3 set-multilinear formula computing f. Such lower bounds are proved in [NW97] for polynomials such as the elementary symmetric polynomial and the determinant.

We conjecture that any polynomial f such that $\dim \partial f$ is small is Möbius-pseudorandom.

Conjecture 4.2. *Suppose $f = \{f_n\}$ is a sequence of integral multilinear polynomials such that $\dim_{\mathbb{Q}} \partial f_n \leq r$ for some "small" r. Then f is Möbius-pseudorandom.*

When r is very small, even a bound on the dimension of the first-order partial derivatives of f can be used to prove Conjecture 4.2.

Theorem 4.3. *Let $f = \{f_n\}_{n\in\mathbb{N}}$ be a sequence of integer polynomials and $r \leq \varepsilon n$ for some small enough constant $\varepsilon > 0$. Suppose that $\dim_{\mathbb{Q}} \left\{ \frac{\partial f_n}{\partial x_i} : 1 \leq i \leq n \right\} \leq r$. Then f is Möbius-pseudorandom.*

In order to prove Theorem 4.3 we need the following lemma.

Lemma 4.4. *Suppose $f \in \mathbb{Z}[\mathbf{x}]$ is a polynomial such that $\dim_{\mathbb{Q}} \left\{ \frac{\partial f}{\partial x_i} : 1 \le i \le n \right\} = r$ for $r \le n$. Then, there exist r linear functions with integral coefficients $\ell_1(\mathbf{x}), \ldots, \ell_r(\mathbf{x})$ and an r-variate polynomial g with integer coefficients such that $f = g(\ell_1(\mathbf{x}), \ldots, \ell_r(\mathbf{x}))$.*

If we only require g and the ℓ_i's to have rational coefficients, this lemma is well known and can be easily proved using a change of basis and partial derivatives computation using the chain rule. Requiring that all coefficients in this expression are integers can be done using a similar proof, but involves a little more care. We will show that the change of basis can be done using a *unimodular* matrix. Recall that a square integer matrix U is unimodular if $\det U \in \{-1, +1\}$. The inverse of U is then also integral.

Claim 4.5. *Suppose $a_1, \ldots, a_n$ are integers such that $\gcd(a_1, \ldots, a_n) = 1$. Then there exists a unimodular $n \times n$ matrix U whose last column is $(a_1, \ldots, a_n)$.*

Proof. For two integers u, v, if $d = \gcd(u, v)$ and p, q are the Bézout coefficients, that is, integers such that $pu + qv = d$, then note that

$$\begin{bmatrix} p & q \\ -v/d & u/d \end{bmatrix} \cdot \begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix},$$

and the matrix on the left has determinant 1. By repeatedly applying this transformation to 2 coordinates (leaving all other coordinates unchanged), starting from the vector $\mathbf{a} = (a_1, \ldots, a_n)$, we can make all coordinates zero except one coordinate (which we may permute to be the last coordinate). That coordinate would equal $\gcd(a_1, \ldots, a_n) = 1$. Thus we found a unimodular matrix U' such that $U'\mathbf{a} = e_n$ where e_n is the n-th elementary basis vector. Letting $U = (U')^{-1}$, $\mathbf{a} = Ue_n$, so $\mathbf{a}$ is the last column of U. Note that U is also unimodular. □

Proof of Lemma 4.4. We use induction on $n - r$. If $r = n$, there is nothing to prove. Suppose $r < n$. Then there are rational constants $c_1, \ldots, c_n$, not all zero, such that

$$\sum_{i=1}^{n} c_i \frac{\partial f}{\partial x_i} = 0.$$

By clearing denominators, we obtain *integers* $a_1, \ldots, a_n$, not all zero, such that

$$\sum_{i=1}^{n} a_i \frac{\partial f}{\partial x_i} = 0. \tag{3}$$

Dividing by their gcd, we may further assume that $\gcd(a_1, \ldots, a_n) = 1$. Let U be a unimodular matrix as in Claim 4.5 and consider

$$h(\mathbf{y}) = f(U\mathbf{y}),$$

where $\mathbf{y} = (y_1, \ldots, y_n)$. Observe that $h \in \mathbb{Z}[\mathbf{y}]$ since f has integer coefficients and U is integral. By the chain rule, and since the last column of U is $\mathbf{a}$,

$$\frac{\partial h}{\partial y_n} = \sum_{i=1}^{n} a_i \frac{\partial f}{\partial x_i}(U\mathbf{y}) = 0.$$

This means that h does not depend on y_n (here we use the assumption that we work over characteristic 0), so h is in fact a polynomial in $n-1$ variables. Further, applying an invertible linear change of variables does not change the dimension of the first order partial derivatives, so the partial derivatives of h still span a space whose dimension is r. By induction,

$$h(y_1, \ldots, y_{n-1}) = g(L_1(\mathbf{y}), \ldots, L_r(\mathbf{y}))$$

for some integral polynomial g and integral linear functions $L_1, \ldots, L_r$, and therefore $\ell_i(\mathbf{x}) = L_i(U^{-1}\mathbf{x})$ is also integral, and

$$g(\ell_1(\mathbf{x}), \ldots, \ell_r(\mathbf{x})) = g(L_1(U^{-1}\mathbf{x}), \ldots, L_r(U^{-1}\mathbf{x})) = h(U^{-1}\mathbf{x}) = f(\mathbf{x}). \qquad \square$$

We can now prove Theorem 4.3.

Proof of Theorem 4.3. Let $\ell_1(\mathbf{x}), \ldots, \ell_r(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$ and $g \in \mathbb{Z}[\mathbf{x}]$ such that $f = g(\ell_1(\mathbf{x}), \ldots, \ell_r(\mathbf{x}))$, as in Lemma 4.4. By considering f modulo 2, which involves reducing the coefficients of g and $\ell_1, \ldots, \ell_r$ modulo 2, it follows that $(-1)^{f(\mathbf{x})}$ depends only on the values of r linear functions modulo 2, so its Fourier-Walsh expansion involves at most 2^r non-zero coefficients. Therefore, by Cauchy-Schwarz, $\left\|(-1)^f\right\|_A \leq 2^{r/2}$. By Lemma 2.3 and by the assumption on r,

$$\left| \frac{1}{N} \sum_{m=0}^{N-1} \mu(m) \exp(i\pi f(m_1, \ldots, m_n)) \right| = o(1)$$

and the result follows. $\square$

Note that since the dimension of first order partial derivatives of f is at most n, Theorem 4.3 is asymptotically optimal (although in general one might expect this dimension to be close to n, even for rather simple polynomials).

4.1 Bounded Depth Algebraic Formulas

An algebraic formula over a field $\mathbb{F}$ is a tree whose leaves are labeled by variables from the set $\{x_1, \ldots, x_n\}$ or constants from $\mathbb{F}$, and every internal node is labeled by either $+$ or $\times$. The formula computes a polynomial in the natural way, and the depth of the formula is the depth of the tree.

Far-reaching extensions of Nisan and Wigderson's basic idea [NW97] were used for proving lower bounds on many algebraic models. Limaye, Srinivasan and Tavenas [LST25] proved super-polynomial lower bounds for bounded-depth algebraic formulas using this technique (see also [For24] for an extension of this result for all fields). These recent works provide directions for extending Conjecture 4.2 in a way that will imply Liouville-pseudorandomness for bounded depth arithmetic circuits.

Conjecture 4.6. *Suppose $f = \{f_n\}$ is a sequence of n-variate integer multilinear polynomials computed by depth-Δ formulas of size s, for $s = poly(n)$ and $\Delta = O(1)$. Then f is Möbius-pseudorandom.*

5 Circuits with Few Multiplication Gates

The results of the previous section extend to circuits with few multiplication gates.

Theorem 5.1. *Suppose $f \in \mathbb{Z}[\mathbf{x}]$ is computed by an integral arithmetic circuit with k multiplication gates (with arbitrary fan-in). Then $\left\|(-1)^f\right\|_A \leq 3^k$.*

Proof. Let C be a circuit computing f. Reduce C modulo 2, and let $y_1, \ldots, y_k$ be the outputs of the k multiplication gates, ordered in topological order. Observe that for every $i \in [k]$ we have that

$$y_i = \prod_{j=1}^{a_i} \ell_{i,j}(\mathbf{x}, y_1, \ldots, y_{i-1}) \tag{4}$$

where $\ell_{i,j}$ is a linear function modulo 2. Further, the output of the circuit, which is f modulo 2, is an affine linear function in $\mathbf{x}, y_1, \ldots, y_k$.

We first expand $(-1)^f$ as a function f_k of $\mathbf{x}, y_1, \ldots, y_k$. Observe that f_k is a single Fourier-Walsh character with coefficient ± 1. We now eliminate $y_k, y_{k-1}, \ldots, y_1$ in order to obtain the Fourier expansion of $(-1)^f$ as a function of $\mathbf{x}$.

For $i = k, k-1, \ldots, 1$, suppose we have obtained a function f_i that depends on $\mathbf{x}$ and $y_i, y_{i-1}, \ldots, y_1$. Whenever a character involves the variable y_i, we write it as $(-1)^{y_i} \cdot (-1)^{\ell'(\mathbf{x}, y_1, \ldots, y_{i-1})}$ for some function $\ell'(\mathbf{x}, y_1, \ldots, y_{i-1})$, and then replace $(-1)^{y_i}$ using the identity

$$(-1)^{y_i} = 1 - 2\prod_{j=1}^{a_i} \frac{1 - (-1)^{\ell_{i,j}(\mathbf{x}, y_1, \ldots, y_{i-1})}}{2} \tag{5}$$

that follows from (4).

The expression on the right hand side of (5) has Fourier-Walsh expansion whose algebra norm is at most 3. Therefore, since the right hand side of (5) multiplies in the worst case every character of f_i, we have that after the replacement, $\|f_{i-1}\|_A \leq 3\|f_i\|_A$.

Since $f_0 = (-1)^f$ and $\|f_k\|_A = 1$, it follows that $\left\|(-1)^f\right\|_A \leq 3^k$. □

As an immediate corollary of Theorem 5.1 and Lemma 2.3, we obtain the following.

Corollary 5.2. *There exists $\varepsilon > 0$ such that for every $f \in \mathbb{Z}[\mathbf{x}]$ computed by an integral arithmetic circuit with $k \leq \varepsilon n$ multiplication gates (with arbitrary fan-in), it holds that f is Möbius-pseudorandom.*

6 Möbius-Pseudorandomness of the Determinant

Let $n := k^2$ be a perfect square, and let $X = (x_{i,j})_{i,j \in [k]}$. The determinant polynomial is defined as $\mathsf{Det}_k = \sum_{\sigma \in S_k} (-1)^{\mathrm{sgn}(\sigma)} \prod_{i=1}^{k} x_{i,\sigma(i)}$. In this section we prove that Det_k is

Möbius-Pseudorandom. Observe that since in Definition 1.8 we only look at the value of the determinant modulo 2, the same proof holds for the permanent.

The idea, as before, is to approximate the sign of the determinant by a function of small algebra norm, and then use Lemma 2.3. The approximation we construct is exact when the kernel has small dimension, and matrices with larger kernels are sufficiently rare to control the approximation error.

Lemma 6.1. *Let* $\mathsf{Det}_k : \mathbb{F}_2^{k\times k} \to \{0,1\}$ *as above. For every* $1 \le t \le k$*, there exists a function* $D_t : \mathbb{F}_2^{k\times k} \to \mathbb{R}$ *such that* $\|D_t\|_A \le 2^{(k+1)t}$ *and* $\|\mathsf{Det}_k - D_t\|_2 = O(2^{-t/2})$.

Proof. For a matrix $X \in \mathbb{F}_2^{k\times k}$ denote by $R(X) = k - \mathsf{rank}(X) = \dim\ker X$. Further, let $Z(X) = |\ker X|$.

For a fixed v, let $Z_v : \mathbb{F}_2^{k\times k} \to \{0,1\}$ be the function that equals 1 when $Xv = 0$ and zero otherwise. We have that

$$Z(X) = \sum_{v\in\mathbb{F}_2^k} Z_v(X)$$

Further, the set $\{X : Xv = 0\}$ is a linear space of matrices, so Z_v is an indicator of a subspace. Therefore, $\|Z_v\|_A = 1$ and $\|Z\|_A \le 2^k$. Define now

$$D_t(X) = \prod_{j=1}^{t} \frac{2^j - Z(X)}{2^j - 1}.$$

D_t is defined such that $D_t(X) = 1$ whenever $Z(X) = 1$ (which means that X is non-singular, that is, $\mathsf{Det}_k(X) = 1$), and $D_t(X) = 0$ whenever $Z(X) = 2^r$ for some $1 \le r \le t$, which means that X has nullity at least 1 and at most t (and in particular, $\mathsf{Det}_k(X) = 0$).

By the submultiplicativity of the algebra norm,

$$\|D_t\|_A \le \prod_{j=1}^{t} \frac{2^j + \|Z\|_A}{2^j - 1} \le 2^{(k+1)t}.$$

As argued above, $D_t(X) = \mathsf{Det}_k(X)$ whenever $R(X) \in \{0,\dots,t\}$. If $R(X) = r > t$, we get that

$$\begin{aligned} |D_t(X)| &= \prod_{j=1}^{t} \frac{2^r - 2^j}{2^j - 1} \le \frac{2^{rt}}{\prod_{j=1}^{t}(2^j - 1)} \\ &= \frac{2^{rt-\binom{t+1}{2}}}{\prod_{j=1}^{t}(1 - 2^{-j})} = O\left(2^{rt-\binom{t+1}{2}}\right), \end{aligned} \tag{6}$$

since $\prod_{j=1}^{t}(1 - 2^{-j})$ is bounded from below by an absolute constant.

Further, for a randomly chosen $X \in \mathbb{F}_2^{k\times k}$ we have that $\Pr[R(X) \ge r] \le O(2^{-r^2})$, as there are $O(2^{r(k-r)})$ subspaces of dimension r, each of which lies in $\ker X$ with probability 2^{-kr}. Finally, we estimate

$$\|\mathsf{Det}_k - D_t\|_2^2 = \mathbb{E}_X[(\mathsf{Det}_k(X) - D_t(X))^2]$$

Conditioning on $R(X) = r$ for $r = 0, \ldots, k$, the error is 0 whenever $r \leq t$ and, by (6), at most $O\left(2^{rt-\binom{t+1}{2}}\right)$ whenever $r \geq t$ (recall that $\mathsf{Det}_k(X) = 0$ in this case), and therefore

$$\|\mathsf{Det}_k - D_t\|_2^2 = O\left(\sum_{r=t+1}^{k} 2^{-r^2+2tr-t(t+1)}\right)$$

Observing that $-r^2 + 2tr - t(t+1) = -t - (t-r)^2$, we get that

$$\|\mathsf{Det}_k - D_t\|_2^2 = O\left(2^{-t}\sum_{s\geq 1} 2^{-s^2}\right) = O(2^{-t}),$$

as required by the lemma. □

Theorem 6.2. *The $k\times k$ determinant polynomial on $n = k^2$ variables, Det_k, is Möbius-pseudorandom.*

Proof. We first set parameters such that the function D_t from Lemma 6.1 is Möbius-pseudorandom by virtue of Lemma 2.3. Indeed, set $t = k^{0.1}$ and let $D := D_t$ as in Lemma 6.1. It then holds that $\|D\|_A \leq 2^{(k+1)t} = 2^{o(n)}$.

To apply Lemma 2.3, we need a bound on $\|D\|_2$. By writing $D = \mathsf{Det}_k + (D - \mathsf{Det}_k)$, it holds by Lemma 6.1 and the triangle inequality that

$$\|D\|_2 \leq \|\mathsf{Det}_k\|_2 + \|D - \mathsf{Det}_k\|_2 \leq 2$$

for large enough n.

Since Lemma 2.3 as stated requires a function of L_2 norm at most 1, we may define $\tilde{D} = D/2$, so that $\left\|\tilde{D}\right\|_2 \leq 1$ and $\left\|\tilde{D}\right\|_A = 2^{o(n)}$. By Lemma 2.3 we therefore get

$$\left|\frac{1}{N}\sum_{m=0}^{N-1}\mu(m)\tilde{D}(m_1, \ldots, m_n)\right| = o(1),$$

which clearly implies the same bound for D.

We now move on to bound the correlation of $(-1)^{\mathsf{Det}_k}$ with the Möbius function. Since Det_k mod 2 is $\{0,1\}$-valued,

$$(-1)^{\mathsf{Det}_k} = 1 - 2\mathsf{Det}_k = 1 - 2(\mathsf{Det}_k - D) - 2D.$$

Letting $E = \mathsf{Det}_k - D$, it therefore follows that

$$\begin{aligned}\left|\frac{1}{N}\sum_{m=0}^{N-1}\mu(m)(-1)^{\mathsf{Det}_k(m_1,\ldots,m_n)}\right| \leq \left|\frac{1}{N}\sum_{m=0}^{N-1}\mu(m)\right| + 2\left|\frac{1}{N}\sum_{m=0}^{N-1}\mu(m)E(m_1,\ldots,m_n)\right| \\ + 2\left|\frac{1}{N}\sum_{m=0}^{N-1}\mu(m)D(m_1,\ldots,m_n)\right|.\end{aligned}$$

The first term above is $o(1)$ by the prime number theorem, and the third one is $o(1)$ by the argument above. As for the second one, by Cauchy-Schwarz we have that

$$\left|\frac{1}{N}\sum_{m=0}^{N-1}\mu(m)E(m_1,\dots,m_n)\right| \le \left(\frac{1}{N}\sum_{m=0}^{N-1}\mu(m)^2\right)^{1/2}\left(\frac{1}{N}\sum_{m=0}^{N-1}E(m_1,\dots,m_n)^2\right)^{1/2}$$
$$\le \left(\frac{1}{N}\sum_{m=0}^{N-1}E(m_1,\dots,m_n)^2\right)^{1/2} = o(1)$$

by Lemma 6.1. □

AI Use Disclosure

The authors used ChatGPT Astra in all stages of this work, including for finding and verifying proofs, help in locating and understanding references, and proofreading.

References

[Bou13a] Jean Bourgain. Möbius-Walsh correlation bounds and an estimate of Mauduit and Rivat. *Journal d'Analyse Mathématique*, 119(1):147–163, 2013.

[Bou13b] Jean Bourgain. On the Fourier-Walsh spectrum of the Moebius function. *Israel J. Math.*, 197(1):215–235, 2013.

[Bou16] Jean Bourgain. On the Fourier-Walsh spectrum of the Moebius function, II. *J. Anal. Math.*, 128:355–367, 2016.

[BSZ12] Jean Bourgain, Peter Sarnak, and Tamar Ziegler. Disjointness of Moebius from horocycle flows. In *From Fourier Analysis and Number Theory to Radon Transforms and Geometry: In Memory of Leon Ehrenpreis*, pages 67–83. Springer, 2012.

[Dav37] Harold Davenport. On some infinite series involving arithmetical functions (II). *The Quarterly Journal of Mathematics*, 8(1):313–320, 1937.

[FKPL18] Sébastien Ferenczi, Joanna Kułaga-Przymus, and Mariusz Lemańczyk. Sarnak's conjecture: what's new. In *Ergodic Theory and Dynamical Systems in their Interactions with Arithmetics and Combinatorics: CIRM Jean-Morlet Chair, Fall 2016*, pages 163–235. Springer, 2018.

[For24] Michael A. Forbes. Low-Depth Algebraic Circuit Lower Bounds over Any Field. In *39th Computational Complexity Conference, CCC 2024*, volume 300 of *LIPIcs*, pages 31:1–31:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.

[Gre12] Ben Green. On (Not) Computing the Möbius Function Using Bounded Depth Circuits. *Combinatorics, Probability and Computing*, 21(6):942–951, 2012.

[GT12] Ben Green and Terence Tao. The Möbius function is strongly orthogonal to nilsequences. *Annals of Mathematics*, 175(2):541–566, 2012.

[Hua65] Loo-Keng Hua. *Additive Theory of Prime Numbers*, volume 13 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1965.

[Kal11] Gil Kalai. The AC^0 Prime Number Conjecture. Combinatorics and More, February 21 2011.

[LST25] Nutan Limaye, Srikanth Srinivasan, and Sébastien Tavenas. Superpolynomial Lower Bounds Against Low-Depth Algebraic Circuits. *J. ACM*, 72(4):26:1–26:35, 2025.

[MR10] Christian Mauduit and Joël Rivat. Sur un problème de Gelfond: la somme des chiffres des nombres premiers. *Ann. of Math. (2)*, 171(3):1591–1646, 2010.

[Mül17] Clemens Müllner. Automatic sequences fulfill the Sarnak conjecture. *Duke Math. J.*, 166(17):3219–3290, 2017.

[NW97] Noam Nisan and Avi Wigderson. Lower Bounds on Arithmetic Circuits Via Partial Derivatives. *Comput. Complex.*, 6(3):217–234, 1997.

[Raz87] Alexander A. Razborov. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Mat. Zametki*, 41:598–607, 1987. English translation in Mathematical Notes of the Academy of Sci. of the USSR, 41(4):333-338, 1987.

[Sar10] Peter Sarnak. Three lectures on the Möbius function, randomness and dynamics, 2010. https://www.math.ias.edu/files/wam/2011/PSMobius.pdf.

[Sar12] Peter Sarnak. Möbius randomness and dynamics. *Not. S. Afr. Math. Soc*, 43(2):89–97, 2012.

[Smo87] Roman Smolensky. Algebraic Methods in the Theory of Lower Bounds for Boolean Circuit Complexity. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing*, pages 77–82. ACM, 1987.

[Smo93] Roman Smolensky. On Representations by Low-Degree Polynomials. In *34th Annual Symposium on Foundations of Computer Science*, pages 130–138. IEEE Computer Society, 1993.

[Tao12] Terence Tao. Answer to "Möbius Randomness of the Rudin-Shapiro Sequence". MathOverflow, September 25 2012.

[Zie26] Tamar Ziegler. Sign patterns of the Liouville function. In *European Congress of Mathematics*, pages 203–215. EMS Press, 2026.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il